

WHAT IS CLAIMED

1 1. A method for controllably encrypting data to be
2 transmitted over a communication path between a data source
3 and a data recipient, comprising the steps of:

4 5 (a) providing a plurality of respectively different
6 data encryption operators, and of which may be used, but
7 none of which is necessarily required to encrypt said data
8 into an unintelligible form for transmission over said
9 communication path;

10 10 (b) passing said data to be transported over said
11 communication path through a first of said respectively
12 different encryption operators to thereby produce a first
13 encrypted data stream; and

14 14 (c) passing said first encrypted data stream through
15 a second selected one of said respectively different data
16 encryption operators to thereby produce a compound
17 encrypted output data stream that is an encryption of said
18 first encrypted data stream.

1 1. A method according to claim 1, further including
2 the steps of:

3 3 (d) transporting said compound encrypted output data
4 stream over said communication path to said data recipient;
5 and

6 (e) passing said output data stream through a
7 sequence of second and first decryption operators that
8 respectively decrypt data that has been encrypted by said
9 second and first encryption operators, so as to recover
10 said data.

1 3. A method according to claim 1, wherein step (a)
2 comprises storing said plurality of respectively different
3 data encryption operators in an encryption operator
4 database, and wherein step (b) comprises retrieving said
5 first encryption operator from said database and passing
6 said data to be transported over said communication path
7 through said retrieved first encryption operator to thereby
8 produce a first encrypted data stream, and step (c)
9 comprises retrieving said second encryption operator from
10 said database and passing said first encrypted data stream
11 through said second encryption operator to thereby produce
12 said compound encrypted output data stream.

1 4. A method according to claim 1, further including
2 the steps of:

3 (d) transporting said compound encrypted output data
4 stream over said communication path to said data recipient;
5 and

6 (e) passing said compound output data stream through
7 a sequence of second and first decryption operators that
8 respectively decrypt data that has been encrypted by said
9 second and first encryption operators, so as to recover
10 said data.

1 5. A method according to claim 4, wherein step (e)
2 comprises storing a plurality of respectively different
3 data decryption operators in a decryption operator
4 database, retrieving from said decryption operator database
5 second and first decryption operators that respectively
6 decrypt data that has been encrypted by said second and
7 first encryption operators, and passing said compound
8 output data stream through a sequence of said second and
9 first decryption operators so as to successively decrypt
10 said compound output data stream and thereby recover said
11 data.

1 6. A method for controllably encrypting data to be
2 transmitted over a communication path between a data source
3 and a data recipient, comprising the steps of:
4

5 (a) providing a plurality of respectively different
6 data encryption operators;

7 (b) sequentially passing data to be transported over
8 said communication path through multiple ones of said
9 respectively different data encryption operators to thereby
produce a compound-encrypted data stream.

1 7. A method according to claim 6, further including
2 the steps of:

3 (c) transporting said compound-encrypted data stream
4 over said communication path to said data recipient; and

5 (d) passing said compound-encrypted data stream
6 through a sequence of multiple decryption operators that
7 sequentially decrypt said compound-encrypted data so as to
recover said data.

1 8. A method for controllably encrypting data to be
2 transmitted over a communication path between a data source
3 and a data recipient, comprising the steps of:

4 (a) storing a plurality of respectively different
5 data encryption operators in a data encryption operator
6 database;

7 (b) retrieving from said database and assembling
8 selected ones of said respectively different data
9 encryption operators into a sequence of data encryption
10 operators, wherein immediately successive ones of said data
11 encryption operations of said sequence are different from
12 one another; and

13 (c) passing data to be transported over said
14 communication path through said sequence of data encryption
15 operators generated in step (b), so as to produce a
16 compound-encrypted data stream.

9. A method according to claim 8, further including the steps of:

(d) transporting said compound-encrypted data stream over said communication path to said data recipient;

(e) retrieving from a decryption operator database in which a plurality of respectively different data decryption operators are stored, respective decryption operators that respectively decrypt data that has been encrypted by said selected encryption operators;

(f) passing said compound-encrypted output data stream through a sequence of decryption operators retrieved in step (e), successively decrypting said compound-encrypted data stream and thereby recover said data.

10. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) providing a plurality of respectively different data encryption operators;

(b) generating a sequence of data encryption operators comprised of plural ones of said respectively different data encryption operators provided in step (a); and

(c) passing data to be transported over said communication path through said sequence of data encryption operators generated in step (b), so as to produce a compound-encrypted output data stream.

~~11. A method according to claim 10, further including the steps of:~~

(d) transporting said compound-encrypted output data stream over said communication path to said data recipient; and

(e) passing said compound-encrypted output data stream through a sequence of decryption operators that respectively decrypt data that has been encrypted by said data encryption operators, so as to recover said data.

12. A method for controllably encrypting data to be transmitted over a communication path between a data source and a data recipient, comprising the steps of:

(a) storing a plurality of respectively different data encryption operators;

(b) generating a sequence of access codes, each of which is associated with a respective one of said data encryption operators stored in step (a), with immediately successive ones of said access codes of said sequence being different from one another;

(c) accessing selected ones of said respectively different data encryption operators stored in step (a) in accordance with said sequence of access codes generated in step (b), so as to produce a sequence of data encryption operators, in which immediately successive ones of said data encryption operators are different from one another; and

(d) passing data to be transported over said communication path through said sequence of data encryption operators produced in step (c) to produce a compound-encrypted data stream.

13. A method according to claim 12, further including the steps of:

(e) transporting said compound-encrypted output data stream over said communication path to said data recipient; and

(f) passing said compound-encrypted output data stream through a sequence of decryption operators that respectively decrypt data that has been encrypted by said data encryption operators, so as to recover said data.

1 14. A system for controllably encrypting data to be
2 transmitted over a communication path between a data source
3 site and a data recipient site, comprising:

4 at said data source site,

5 a data encryption operator database which stores a
6 plurality of respectively different data encryption
7 operators;

8 an address code generator which generates a sequence
9 of access codes, each of which is associated with a
10 respective one of said data encryption operators stored in
11 said data encryption database, such that immediately
12 successive ones of said access codes of said sequence
13 differ from one another, so as to access from said data
14 encryption operator database a sequence of stored data
15 encryption operators, such that immediately successive ones
16 of retrieved data encryption operators are different from
17 one another; and

18 a signal processor which is operative to apply data to
19 be transported over said communication path through said
20 sequence of data encryption operators accessed from said
21 encryption operator database to produce a compound-
22 encrypted data stream for transport over said communication
23 path.

1 15. A system according to claim 14, further
2 including, at said data recipient site,

3 a data decryption operator database which stores a
4 plurality of respectively different data decryption
5 operators;

6 an address code generator which generates a sequence
7 of access codes, each of which is associated with a
8 respective one of said data decryption operators stored in
9 said data decryption database, and is operative to cause a
10 sequence of data decryption operators to be accessed from
11 said data decryption database in accordance with the
12 reverse order of said sequence of data encryption operators
13 that produced said compound-encrypted data stream; and

14 a signal processor which is operative to apply said
15 compound-encrypted data stream that has been transported
16 over said communication path to said data recipient site
17 through said sequence of data encryption operators accessed
18 from said encryption operator database to recover said
19 data.